Gabriel Henrique **Lopes Gomes Alves Nunes**

Doutorando em Ciência da Computação | MSc Ciência da Computação, BSc Física

nunesgh.com · nunesgh.com/scholar · nunesgh.com/orcid · nunesgh.com/lattes

Sydney, New South Wales, Austrália

Doutorando em Cotutela em Ciência da Computação na Universidade Federal de Minas Gerais (UFMG), Brasil, e na Macquarie University, Austrália. Mestre em Ciência da Computação e Bacharel em Física pela UFMG. Interessado em Métodos Formais, Fluxo de Informação Quantitativo, Computação Responsável (e.g. Privacidade, Utilidade, Justiça), Inteligência Artificial, e Neurociência.

Membro do Topete Research Group e do Laboratório INSCRYPT | T-Rex.

Educação

02/2023 – 06/2025 Doutorado em Ciência da Computação com bolsa *International Macquarie University Research Excellence Scholarship* (iMQRES) na School of Computing da Macquarie University (Researcher Profile). Orientado em Cotutela pela Prof. Annabelle McIver.

07/2021 – 06/2025 Doutorado em Ciência da Computação com Bolsa CAPES no Programa de Pós-Graduação em Ciência da Computação da UFMG. Orientado em Cotutela pelo Prof. Mário Alvim.

- Área de pesquisa: Teoria do Fluxo de Informação Quantitativo e aplicações para caracterizar precisamente como diferentes métodos de introdução de ruído afetam o equilíbrio entre privacidade e utilidade em microdados e em publicações de dados estatísticos.

03/2019 – 04/2021 Mestrado em Ciência da Computação com Bolsa CNPq no Programa de Pós-Graduação em Ciência da Computação da UFMG. Orientado pelo Prof. Mário Alvim e pela Prof. Annabelle McIver.

- Dissertação defendida e aprovada em 28 de abril de 2021: A formal quantitative study of privacy in the publication of official educational censuses in Brazil (**HDL**: 1843/38085).
- Dissertação selecionada para o XXXV Concurso de Teses e Dissertções (CTD 2022), parte do XLII Congresso da Sociedade Brasileira de Computação (CSBC 2022) (**DOI**: 10.5753/ctd.2022.223158).

03/2014 – 07/2018 Bacharelado em Física na UFMG.

03/2012 – 12/2013 Bacharelado em Nanotecnologia na Universidade Federal do Rio de Janeiro. Incompleto.

02/2011 – 06/2011 Bacharelado em Medicina na Ciências Médicas de Minas Gerais. Incompleto.

Experiência

07/2023 – 06/2025 **Sessional Teaching Academic, Macquarie University, Sydney, New South Wales, Australia**
Offensive Security (COMP2320/COMP6320), Data Privacy and Information Security (COMP3300), Secure Applications Development (COMP3310), and Formal Methods (COMP4000) at the School of Computing.
Computer Science | Ethical Hacking | Formal Methods | Java | Privacy | Python | Quantitative Information Flow | Security

07/2022 – 11/2022 **Student Researcher, Google LLC, New York, New York, USA**
Estágio orientado por Dr. Andrés Muñoz Medina.
Ciência da Computação | Apache Beam | Machine Learning | Fluxo de Informação Quantitativo | Privacidade | Python

12/2020 – 03/2021 **Analista de Segurança da Informação, Fundação de Desenvolvimento da Pesquisa, UFMG, Belo Horizonte, Minas Gerais, Brasil**
Analista de Segurança da Informação no projeto PRICE - Privacidade em Censos Educacionais.
Ciência da Computação | Privacidade | Python | Fluxo de Informação Quantitativo | Transparência

09/2019 – 11/2019 **Visiting Scholar, Macquarie University, Sydney, New South Wales, Australia**
Estágio no Departamento de Computação. Orientado pela Prof. Annabelle McIver.
Ciência da Computação | Privacidade | Python | Fluxo de Informação Quantitativo | Transparência

03/2019 – Presente **Administrador de Sistema de TI Voluntário, UFMG, Belo Horizonte, Minas Gerais, Brasil**
Laboratório INSCRYPT | T-Rex.
Ciência da Computação | Linux | Debian | Administração de Sistema | Voluntariado

01/2016 – 10/2014 **Monitoria & Iniciação Tecnológica e Industrial na Sala de Demonstrações de Física, UFMG, Belo Horizonte, Minas Gerais, Brasil**

- Desenvolvimento: espectrômetro óptico de alta resolução e baixo custo e Armadilha de Paul elétrica.
- Bolsista PROGRAD/UFMG & CNPq. Orientado pelo Prof. Elmo Salomão.

Física | Espectrômetro | LabVIEW | SolidWorks

Premiações

Excellence in Higher Degree Research (Student Award) — Dezembro de 2024
Faculty of Science and Engineering, Macquarie University.

Outstanding Poster — Junho de 2024
Future Communications Research Centre, Macquarie University.
Poster: Quantitative Information Flow for Privacy Analysis (Future Communications Research Centre Workshop).

Ciência da Computação | Topics API | Cookies de Terceiros | Fluxo de Informação Quantitativo | Equilíbrio entre Privacidade e Utilidade

Research Rising Star — Outubro de 2023
School of Computing, Faculty of Science and Engineering, Macquarie University.
Paper: A Novel Analysis of Utility in Privacy Pipelines, Using Kronecker Products and Quantitative Information Flow.

Ciência da Computação | Privacidade | Equilíbrio entre Privacidade e Utilidade | Fluxo de Informação Quantitativo

Google LARA Research Scholarship — Fevereiro de 2022
9th Google Latin America Research Awards (LARA).
Uma estrutura robusta e explicável baseada em QIF para avaliar os riscos de privacidade de grandes dados.

Ciência da Computação | Fluxo de Informação Quantitativo | Controle de Divulgação | Microdados | Privacidade Diferencial | Privacidade

Artigos de Conferência

The Privacy-Utility Trade-off in the Topics API — Outubro de 2024
2024 ACM SIGSAC Conference on Computer and Communications Security. DOI: 10.1145/3658644.3670368. arXiv: 2406.15309.
The ongoing deprecation of third-party cookies by web browser vendors has sparked the proposal of alternative methods to support more privacy-preserving personalized advertising on web browsers and applications. The Topics API is being proposed by Google to provide third-parties with "coarse-grained advertising topics that the page visitor might currently be interested in". In this paper, we analyze the re-identification risks for individual Internet users and the utility provided to advertising companies by the Topics API, i.e. learning the most popular topics and distinguishing between real and random topics. We provide theoretical results dependent only on the API parameters that can be readily applied to evaluate the privacy and utility implications of future API updates, including novel general upper-bounds that account for adversaries with access to unknown, arbitrary side information, the value of the differential privacy parameter ϵ, and experimental results on real-world data that validate our theoretical model.
Co-authors: Prof. Mário Alvim, Natasha Fernandes, Prof. Annabelle McIver.

Ciência da Computação | Topics API | Cookies de Terceiros | Fluxo de Informação Quantitativo | Privacidade | Utilidade | Privacidade Diferencial

A Novel Analysis of Utility in Privacy Pipelines, Using Kronecker Products and Quantitative Information Flow — Novembro de 2023
2023 ACM SIGSAC Conference on Computer and Communications Security. DOI: 10.1145/3576915.3623081. arXiv: 2308.11110.
We combine Kronecker products, and quantitative information flow, to give a novel formal analysis for the fine-grained verification of utility in complex privacy pipelines. The combination explains a surprising anomaly in the behaviour of utility of privacy-preserving pipelines - that sometimes a reduction in privacy results also in a decrease in utility. We use the standard measure of utility for Bayesian analysis, introduced by Ghosh at al., to produce tractable and rigorous proofs of the fine-grained statistical behaviour leading to the anomaly. More generally, we offer the prospect of formal-analysis tools for utility that complement extant formal analyses of privacy. We demonstrate our results on a number of common privacy-preserving designs.
Co-authors: Prof. Mário Alvim, Natasha Fernandes, Prof. Annabelle McIver, Prof. Carroll Morgan.

Ciência da Computação | Fluxo de Informação Quantitativo | Privacidade | Utilidade | Equilíbrio entre Privacidade e Utilidade | Privacidade Diferencial

Measuring Re-identification Risk — Junho de 2023
2023 ACM SIGMOD/PODS Conference. DOI: 10.1145/3589294. arXiv: 2304.07210.
Compact user representations (such as embeddings) form the backbone of personalization services. In this work, we present a new theoretical framework to measure re-identification risk in such user representations. Our framework, based on hypothesis testing, formally bounds the probability that an attacker may be able to obtain the identity of a user from their representation. As an application, we show how our framework is general enough to model important real-world applications such as the Chrome's Topics API for interest-based advertising. We complement our theoretical bounds by showing provably good attack algorithms for re-identification that we use to estimate the re-identification risk in the Topics API. We believe this work provides a rigorous and interpretable notion of re-identification risk and a framework to measure it that can be used to inform real-world applications.
Co-authors: CJ Carey, Travis Dick, Alessandro Epasto, Adel Javanmard, Josh Karlin, Shankar Kumar, Andres Muñoz Medina, Vahab Mirrokni, Sergei Vassilvitskii, Peilin Zhong.

Ciência da Computação | Risco de re-identificação | Privacidade | Representações de Usuários

Flexible and scalable privacy assessment for very large datasets, with an application to official governmental microdata — Julho de 2022
22nd Privacy Enhancing Technologies Symposium (PETS 2022). DOI: 10.56553/popets-2022-0114.
Apresentamos uma refatoração sistemática do tratamento convencional de análises de privacidade, baseando-o em conceitos matemáticos do framework de Fluxo de Informação Quantitativo (QIF). A abordagem que sugerimos traz três vantagens principais: é flexível, permitindo quantificar e comparar com precisão os riscos de privacidade para ataques conhecidos e novos; pode ser computacionalmente tratável para conjuntos de dados longitudinais muito grandes; e seus resultados são explicáveis tanto para os políticos quanto para o público em geral. Aplicamos nossa abordagem a um estudo de caso muito grande: os Censos Educacionais do Brasil, com curadoria da agência governamental INEP, que compreende mais de 90 atributos de aproximadamente 50 milhões de indivíduos divulgados longitudinalmente todos os anos desde 2007. Esses conjuntos de dados só muito recentemente (2018-2021) atraíram legislação para regular sua privacidade - ao mesmo tempo em que continuam mantendo a abertura que se buscava na sociedade brasileira. A reação do INEP a essa legislação foi a gênese do nosso projeto com eles. Em nossas conclusões aqui compartilhamos as lições científicas, técnicas e de comunicação que aprendemos no processo.
Coautores: Prof. Mário Alvim, Natasha Fernandes, Prof. Annabelle McIver, Prof. Carroll Morgan.

Ciência da Computação | Fluxo de Informação Quantitativo | Controle de Divulgação | Microdados | Privacidade

A formal quantitative study of privacy in the publication of official educational censuses in Brazil — Abril de 2021

Universidade Federal de Minas Gerais. DOI: hdl:1843/38085.

Nesta dissertação, fornecemos um estudo quantitativo completo dos riscos à privacidade na divulgação dos Censos Educacionais Brasileiros oficiais fornecidos anualmente pelo INEP, que é o órgão governamental brasileiro responsável pelo desenvolvimento e manutenção de sistemas de estatísticas educacionais. Mais precisamente, analisamos formalmente os riscos de privacidade em bancos de dados divulgados como microdados, i.e. dados no nível de registro de cada indivíduo, e protegidos pela técnica de desidentificação, i.e. a remoção de informações de identificação direta, como nomes de indivíduos ou números de identificação pessoal.

Ciência da Computação | Fluxo de Informação Quantitativo | Controle de Divulgação | Microdados | Privacidade | Utilidade | Privacidade Diferencial

On Privacy and Accuracy in Data Releases — Agosto de 2020

31st International Conference on Concurrency Theory (CONCUR 2020). DOI: 10.4230/LIPIcs.CONCUR.2020.1.

Neste artigo, estudamos a relação entre privacidade e acurácia no contexto de conjuntos de dados correlacionados. Usamos um modelo de fluxo de informação quantitativo para descrever o equilíbrio entre a privacidade dos dados dos indivíduos e a utilidade das consultas a esses dados, modelando a eficácia dos adversários que tentam fazer inferências após a divulgação dos dados. Mostramos que, onde existem correlações em conjuntos de dados, não é possível implementar mecanismos de adição de ruído ideais que forneçam a melhor precisão possível ou a melhor privacidade possível em todas as situações. Finalmente, ilustramos o equilíbrio entre precisão e privacidade para mecanismos de privacidade diferencial local e *oblivious* em termos de ataques de inferência em conjuntos de dados de média escala.

Coautores: Prof. Mário Alvim, Natasha Fernandes, Prof. Annabelle McIver.

Ciência da Computação | Equilíbrio entre Privacidade e Utilidade | Fluxo de Informação Quantitativo | Ataques de Inferência | Privacidade Diferencial

Software

Topics API Analysis — Junho de 2024

Zenodo. DOI: 10.5281/ZENODO.11032230.

This repository provides the experimental results of the paper *The Privacy-Utility Trade-off in the Topics API* (DOI: 10.1145/3658644.3670368; arXiv: 2406.15309).

Software | Topics API | Cookies de Terceiros | Fluxo de Informação Quantitativo | Privacidade | Utilidade | Padrões da Web

Bayes Vulnerability for Microdata (BVM) library — Abril de 2021

Zenodo. DOI: 10.5281/zenodo.6533703.

Quantitative Information Flow assessment of vulnerability for microdata datasets using Bayes Vulnerability. This tool was used for the vulnerability assessment published in: *A formal quantitative study of privacy in the publication of official educational censuses in Brazil* (hdl:1843/38085) and *Flexible and scalable privacy assessment for very large datasets, with an application to official governmental microdata* (DOI: 10.56553/popets-2022-0114, arXiv: 2204.13734).

Software | Privacidade | Utilidade | Métodos Formais | Fluxo de Informação Quantitativo

Datasets

AOL Dataset for Browsing History and Topics of Interest — June 2024

Zenodo. DOI: 10.5281/zenodo.11029571.

This record provides the datasets of the paper *The Privacy-Utility Trade-off in the Topics API* (DOI: 10.1145/3658644.3670368; arXiv: 2406.15309). The datasets generating code and the experimental results can be found in 10.5281/zenodo.11229402 (nunesgh/topics-api-analysis).

Dataset | Topics API | Cookies de Terceiros | Fluxo de Informação Quantitativo | Privacidade | Utilidade | Publicidade Baseada em Interesses

Publicações Acadêmicas

A formal quantitative study of privacy in the publication of official educational censuses in Brazil — Abril de 2021

Universidade Federal de Minas Gerais. HDL: hdl:1843/38085.

Nesta dissertação, fornecemos um estudo quantitativo completo dos riscos à privacidade na divulgação dos Censos Educacionais Brasileiros oficiais fornecidos anualmente pelo INEP, que é o órgão governamental brasileiro responsável pelo desenvolvimento e manutenção de sistemas de estatísticas educacionais. Mais precisamente, analisamos formalmente os riscos de privacidade em bancos de dados divulgados como microdados, i.e. dados no nível de registro de cada indivíduo, e protegidos pela técnica de desidentificação, i.e. a remoção de informações de identificação direta, como nomes de indivíduos ou números de identificação pessoal.

Ciência da Computação | Fluxo de Informação Quantitativo | Controle de Divulgação | Microdados | Privacidade Diferencial | Privacidade | Utilidade

An Introduction to Raman Spectroscopy — Novembro de 2017

Material didático ou instrucional.

As aplicações da Espectroscopia Raman são vastas na Física, Química, Geologia e em outras áreas, uma vez que é possível caracterizar diferentes materiais através de seus espectros vibracionais. Esse é um método eficiente e não destrutivo, logo útil não apenas em um laboratório, mas também para alguns problemas cotidianos. Neste estudo, parte da teoria clássica da Espectroscopia Raman deve ser desenvolvida de modo que possa ser aplicada a um caso específico em um exemplo experimental. Ao fim deste estudo, todas as ideias básicas por trás da técnica da Espectroscopia Raman serão abordadas.

Orientado pelo Prof. Leandro Malard.

Física | Espectroscopia Raman

Uma Introdução Geométrica aos Grupos de Lie — Novembro de 2016

III Simpósio Nacional do Programa de Iniciação Científica e Mestrado (PICME).

Coautores: André Nascimento, Cássio Feitosa, Cleber Barreto, Diego Carriel. Orientado por Romero Solha.

Matemática | Grupos de Lie

Artigos de Workshop

A new Framework for Measuring Re-Identification Risk — Dezembro de 2023

Workshop on Regulatable Machine Learning at the 37th Conference on Neural Information Processing Systems (RegML @ NeurIPS 2023).

Compact user representations (such as embeddings) form the backbone of personalization services. In this work, we present a new theoretical framework to measure re-identification risk in such user representations. Our framework, based on hypothesis testing, formally bounds the probability that an attacker may be able to obtain the identity of a user from their representation. As an application, we show how our framework is general enough to model important real-world applications such as the Chrome's Topics API for interest-based advertising. We complement our theoretical bounds by showing provably good attack algorithms for re-identification that we use to estimate the re-identification risk in the Topics API. We believe this work provides a rigorous and interpretable notion of re-identification risk and a framework to measure it that can be used to inform real-world applications.

Co-authors: CJ Carey, Travis Dick, Alessandro Epasto, Adel Javanmard, Josh Karlin, Shankar Kumar, Andres Muñoz Medina, Vahab Mirrokni, Sergei Vassilvitskii, Peilin Zhong.

Ciência da Computação | Risco de re-identificação | Privacidade | Representações de Usuários

A Quantitative Information Flow Analysis of the Topics API — November 2023

Proceedings of the 22nd Workshop on Privacy in the Electronic Society (WPES 2023). DOI: 10.1145/3603216.3624959.

Third-party cookies have been a privacy concern since cookies were first developed in the mid 1990s, but more strict cookie policies were only introduced by Internet browser vendors in the early 2010s. More recently, due to regulatory changes, browser vendors have started to completely block third-party cookies, with both Firefox and Safari already compliant. The Topics API is being proposed by Google as an additional and less intrusive source of information for interest-based advertising (IBA), following the upcoming deprecation of third-party cookies. Initial results published by Google estimate the probability of a correct re-identification of a random individual would be below 3% while still supporting IBA. In this paper, we analyze the re-identification risk for individual Internet users introduced by the Topics API from the perspective of Quantitative Information Flow (QIF), an information- and decision-theoretic framework. Our model allows a theoretical analysis of both privacy and utility aspects of the API and their trade-off, and we show that the Topics API does have better privacy than third-party cookies. We leave the utility analyses for future work.

Co-authors: Prof. Mário Alvim, Natasha Fernandes, Prof. Annabelle McIver.

Ciência da Computação | Topics API | Cookies de Terceiros | Fluxo de Informação Quantitativo | Privacidade | Utilidade

A novel analysis of utility in privacy pipelines, using Kronecker products and quantitative information flow — September 2023

Theory and Practice of Differential Privacy (TPDP) 2023.

We combine Kronecker products, and quantitative information flow, to give a novel formal analysis for the fine-grained verification of utility in complex privacy pipelines. The combination explains a surprising anomaly in the behaviour of utility of privacy-preserving pipelines - that sometimes a reduction in privacy results also in a decrease in utility. We use the standard measure of utility for Bayesian analysis, introduced by Ghosh at al., to produce tractable and rigorous proofs of the fine-grained statistical behaviour leading to the anomaly. More generally, we offer the prospect of formal-analysis tools for utility that complement extant formal analyses of privacy. We demonstrate our results on a number of common privacy-preserving designs.

Co-authors: Prof. Mário Alvim, Natasha Fernandes, Prof. Annabelle McIver, Prof. Carroll Morgan.

Ciência da Computação | Fluxo de Informação Quantitativo | Privacidade | Utilidade | Equilíbrio entre Privacidade e Utilidade | Privacidade Diferencial

Measuring Re-identification Risk — May 2023

2023 Security for the Web Workshop.

Compact user representations (such as embeddings) form the backbone of personalization services. In this work, we present a new theoretical framework to measure re-identification risk in such user representations. Our framework, based on hypothesis testing, formally bounds the probability that an attacker may be able to obtain the identity of a user from their representation. As an application, we show how our framework is general enough to model important real-world applications such as the Chrome's Topics API for interest-based advertising. We complement our theoretical bounds by showing provably good attack algorithms for re-identification that we use to estimate the re-identification risk in the Topics API. We believe this work provides a rigorous and interpretable notion of re-identification risk and a framework to measure it that can be used to inform real-world applications.

Co-authors: CJ Carey, Travis Dick, Alessandro Epasto, Adel Javanmard, Josh Karlin, Shankar Kumar, Andres Muñoz Medina, Vahab Mirrokni, Sergei Vassilvitskii, Peilin Zhong.

Ciência da Computação | Risco de re-identificação | Privacidade | Representações de Usuários

Eventos

- 2024 ACM SIGSAC Conference on Computer and Communications Security — 2024
  CCS — *Symposium, Salt Lake City, UT, U.S.A.*
- 22º Privacy Enhancing Technologies Symposium (YouTube) — 2022
  PoPETs/PETS — *Simpósio. Sydney, NSW, Australia, e Online.*
- 9ª Escola de Verão em Computação do Departamento de Ciência da Computação (PDF) (YouTube) — 2020
  Universidade Federal de Minas Gerais — *Seminário. Belo Horizonte, MG, Brasil.*
- 8ª Escola de Verão em Computação do Departamento de Ciência da Computação — 2019
  Universidade Federal de Minas Gerais — *Seminário. Belo Horizonte, MG, Brasil.*
- VII Escola de Verão em Computação do Departamento de Ciência da Computação — 2018
  Universidade Federal de Minas Gerais — *Seminário. Belo Horizonte, MG, Brasil.*
- III Simpósio Nacional do Programa de Iniciação Científica e Mestrado (PICME) (PDF) — 2016
  Universidade Federal de Minas Gerais — *Simpósio. Belo Horizonte, MG, Brasil.*
- X Escola do Centro Brasileiro de Pesquisas Físicas (CBPF) — 2015
  Centro Brasileiro de Pesquisas Físicas — *Seminário. Rio de Janeiro, RJ, Brasil.*
- XXV Escola de Física do Curso de Pós-Graduação do Departamento de Física — 2014
  Universidade Federal de Minas Gerais — *Seminário. Belo Horizonte, MG, Brasil.*

Projetos

PRICE - Privacidade em Censos Educacionais
2020 - 2021

PRICE INSCRYPT Analista de Segurança da Informação

A Lei Geral de Proteção de Dados Pessoais responsabiliza juridicamente as entidades pela qualidade, confidencialidade e privacidade dos dados sobre indivíduos por elas armazenadas. O INEP, instituto de pesquisa do Ministério de Educação, publica anualmente dados educacionais muito detalhados. O projeto PRICE foi um estudo encomendado pelo INEP sobre como transformar os dados a serem publicados de forma que a privacidade dos alunos não seja violada, mas mantendo sua utilidade para pesquisas estatísticas.

Produção Técnica:

- Produto 01: Relatório sobre o panorama internacional e o contexto do INEP a respeito dos métodos de tratamento de controle de privacidade na divulgação estatística.
- Produto 02: Relatório sobre os riscos à privacidade decorrentes da atual forma de divulgação dos microdados dos Censos Educacionais do INEP.
- Produto 03: Relatório técnico sobre métodos de tratamento aplicáveis aos microdados de divulgação dos Censos Educacionais do INEP.
- Produto 04: Solução tecnológica e sua documentação.
- Produto 05: Relatório técnico final do projeto piloto.
- Produto 06: Relatório técnico de implantação.
- Produto 07: Relatório de operação assistida.
- Produto 08: Relatório de encerramento do projeto.

Termo de Execução Descentralizada (TED) INEP-UFMG 8750.
Coordenador: Prof. Mário Alvim.

Ciência da Computação | Privacidade | Transparência | Python

Workshop sobre técnicas de anonimização de bases de dados
30 de novembro de 2018

Diretoria de Estatísticas Educacionais (DEED/INEP)
Centro de Desenvolvimento e Planejamento Regional (CEDEPLAR/UFMG)

O workshop visa apresentar aos profissionais do INEP o estado da arte das técnicas de anonimização de dados com uso mais recorrente, sua vantagens e desvantagens, de maneira a subsidiar decisões organizacionais em relação a adoção de uma ou mais técnicas, considerando a capacidade técnica das equipes, de infraestrutura, de operação e eventuais limitações jurídicas existentes.
Coordenador: Prof. Mário Alvim.

Ciência da Computação | Privacidade | Transparência

Espectrômetro Óptico Lumus Max
2014 - 2015

Lumus Max Sala de Demonstrações de Física

Desenvolvimento de um espectrômetro óptico de alta resolução e baixo custo. Partes do hardware foram desenvolvidas utilizando-se o software SolidWorks, da Dassault Systèmes, e o software foi implementado utilizando-se a linguagem de programação visual LabVIEW, da National Instruments.
Coordenador: Prof. Elmo Salomão.

Física | Espectrômetro | LabVIEW | SolidWorks

Electrical Paul's Trap
2014 - 2015

Armadilha de Paul Elétrica Sala de Demonstrações de Física

Desenvolvimento de um Armadilha de Paul elétrica (armadilha de íons em quadrupolo).
Coordenador: Prof. Elmo Salomão.

Física